UNIVERSITY COLLEGE TATI

UNIVERSITY COLLEGE TATI (UC TATI)

FINAL EXAMINATION QUESTION BOOKLET

COURSE CODE	:	BNS 3233
COURSE	:	CRYPTOGRAPHY
SEMESTER/SESSION	:	1-2022/2023
DURATION	:	3 HOURS

Instructions:

1. This booklet contains **5** questions. Answer **ALL** questions.
2. All answers should be hand written on your own answer booklet.
3. Write legibly draw sketches wherever required.
4. If doubt, raise your hands and ask the invigilator.

DO NOT OPEN THIS BOOKLET UNTIL YOU ARE TOLD TO DO SO

THIS BOOKLET CONTAINS 6 PRINTED PAGES INCLUDING COVER PAGE

QUESTION 1

a) List **THREE (3)** independent dimensions of cryptography. (3 marks)

b) Describe information protection by cryptography.

i) Integrity (2 marks)

ii) Authenticity (2 marks)

iii) Confidentiality (2 marks)

c) Differentiate **TWO (2)** characteristics between Symmetric and Asymmetric-key encryption. (4 marks)

d) Define Hash Function. State **ONE (1)** reason why it has been called as one-way Hash Function. (4 marks)

QUESTION 2

a) State **TWO (2)** examples of Classical Cryptography using these technique:

i) Substitution (2 marks)

ii) Transposition (2 marks)

c) Find a plaintext with the word of ciphertext: "Z-S-V-E-P" using the shift cipher X with the key of 4. Assume that A=0, B=2… Z=25.

i) Show your work to find plaintext. (5 marks)

ii) Name the type of operations used for transforming plaintext to ciphertext by cipher X. (1 mark)

d) After the Infinity War, where the Avengers lost his battle, Mr Stark got stuck in space and need to returned to the Earth. Mr Stark wishes to send a secret message for help to his teammates. If we assign numeric values to the uppercase alphabet (A=0, B=2… Z=25), the key is "XYJBTMKAOPLIUE".

Use One Time Pad Cipher to analyse the "secret message" (Plaintext) by decrypting the ciphertext; ECUMH NBOHWPZ. (6 marks)

QUESTION 3

a) In Diffie-Hellman Key Exchange Agreement, Anna and Elsa each independently choose secret keys, SA and SE respectively. Anna then computes her public key, PK_A, by raising g to SA and then taking mod p. Elsa similarly computes her own public key PK_E by raising g to SE and then taking mod p. Anna and Elsa then exchange their public keys over the internet. Anna then calculates the shared secret key S1 by raising PK_E to SA and then taking mod p. Similarly, Elsa calculates shared key S2 by raising PK_A to SE and then taking mod p.

i) With p=7 and g=23, suppose Anna and Elsa choose private keys SA=3 and SE=6, respectively. Calculate Anna's and Elsa's public keys, PK_A and PK_E. Show all work. (7 marks)

ii) Following up on part (a)(i), now calculate S1=S2 as the shared symmetric key. Show all work. (6 marks)

b) Analyze **FIVE (5)** steps of key generation of RSA.

i) Show and elaborate the steps of RSA (10 marks)

ii) Which key should be published and kept secret (2 marks)

QUESTION 4

a) Given a=662, b= 414. Solve GCD (a, b) by using Euclidean's Algorithm. (9 marks)

b) Find integers s and t by solving using Extended Euclidean's Algorithm. Such that, GCD (a, b) = s a + t b. (8 marks)

QUESTION 5

a) List **TWO (2)** examples of stream cipher for Symmetric-Key Cryptography. (2 marks)

b) Despite being weak on its own substitution and transposition are still used in the design of modern cryptography. Give **FOUR (4)** examples substitution and transposition that being applied in any modern cryptography. (4 marks)

c) Figure 1 shows that Data Encryption Standard (DES) inner function. Explain **ONE (1)** reason why does DES need an expansion permutation. (2 marks)

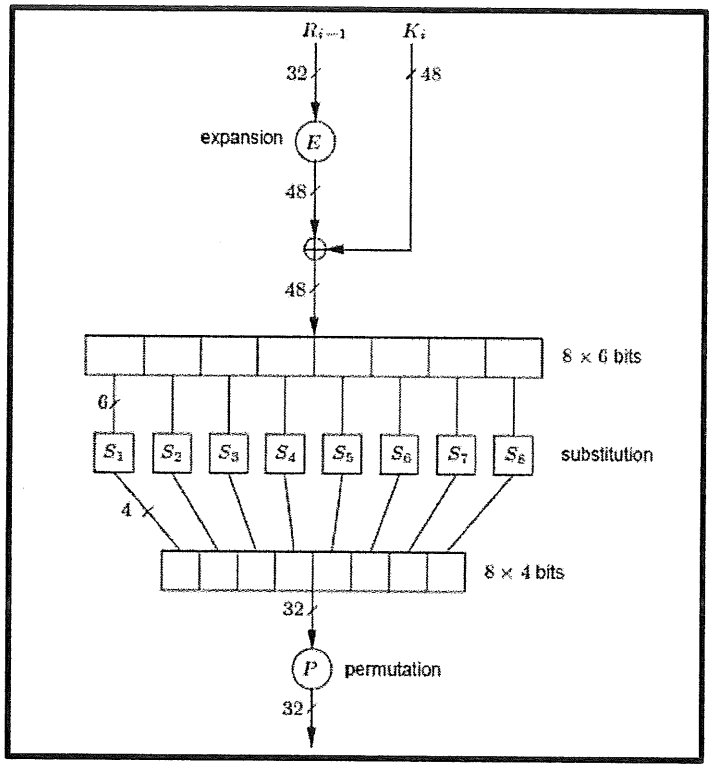

Figure 1: Inner Function of DES algorithm

d) Answer following question based on Table 1

Table 1: S-Box in DES algorithm

mn	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	S_1															
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	3	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	13	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
	S_2															
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
	S_3															
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
	S_4															
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

Table 1 shows S-box of DES algorithm. In DES algorithm, T" ← ($S_1(B_1)$, $S_2(B_2)$, ... $S_8(B_8)$). $S_i(B_i)$ maps B_i to the entry in row and column of Si. Show the result of passing 010011 passing S-Box 4 by answering following questions:

i) What is the value of row in decimal? (2 marks)

ii) What is the value of column in decimal? (2 marks)

iii) By referring S-Box (using your answer in (i) and (ii)), what is the value of output? (1 mark)

e) Advanced Encryption Standard (AES) has four stages which are AddRoundKey, SubByte, ShiftRow and MixColumn. State on which stage that provide:

i) Diffusion (1 mark)

ii) Confusion (1 mark)

f) Figure 2 shows the output of after ShiftRow. Illustrate a diagram before ShiftRow is operating. (4 marks)

A	E	I	M
B	F	J	N
C	G	K	O
D	H	L	P

Figure 2: Output after ShiftRow

g) MixColumn in AES operates on the state column-by-column treating each column as a 4-term polynomial $a(x) = a_3x^3 + a_2x^2\ a_1x^1 + a_0$.

i) Solve ({02}.C3) into a polynomial format. (3 marks)

ii) By answering question (i), divided your answer with irreducible polynomial $x^8+x^4+x^3+x+1$. Write your last answer in binary. (3 marks)

----------End of questions----------